

Transport- och kommunikationsverket Traficom

Guide för domännamnsförmedlare

Anvisningar och krav för den som planerar att bli förmedlare av fi-domännamn

Version 2.0 | juni 2026

Version	Datum	Beskrivning/ändring	Författare
1.0	25.10.2018	Version 1 - ursprunglig publikation	Ari-Matti Husa
1.1	21.12.2018	Version 1.1	Ari-Matti Husa
1.2	6.9.2021	Uppdateringar av KATAKRI-kraven (2.10.4)	Sami Salmensuu
1.3	15.12.2023	Uppdateringar av förmedlarens dataskyddsskyldigheter (2.7)	Mervi Malinen
1.4	19.1.2024	Uppdatering om begränsningar för förmedlare utanför EU/EES-området (2.7.1)	Mervi Malinen
1.5	18.1.2026	Uppdaterade priser (1.1.1)	Sami Salmensuu
1.6	17.2.2026	Inledning tillagd; bilagorna A, B och C	Sami Salmensuu
2.0	15.6.2026	Strukturella och visuella förbättringar Innehållsmässiga tillägg och ändringar i alla avsnitt. Tillgänglighetskorrigeringar.	Sami Salmensuu

Observera

Denna guide är ett vägledande dokument. Det slutliga juridiska ansvaret för att förmedlingsverksamheten är lagenlig ligger alltid hos domännamnsförmedlaren själv.

Aktuell lagstiftning och Traficoms föreskrifter finns på adressen traficom.fi.

Innehållsförteckning

Inledning	4
1 Domännamnsförmedlarens uppgifter och skyldigheter	4
1.1 Domännamnsförmedlarens serviceskyldigheter och priser	5
1.1.1 Betalning för registrering och förnyelse	5
1.2 Skyldighet att ge kunderna råd	5
1.2.1 Minimikrav på rådgivningen.....	5
1.3 Att se till att uppgifterna är korrekta och aktuella	7
1.3.1 Uppdatering av kontaktuppgifter	7
1.3.2 Lagstadgad processadress	7
1.4 Förnyelse av domännamn	8
1.4.1 Förmedlarens skyldigheter när giltighetstiden löper ut.....	8
1.5 Uppsägning av domännamn	8
1.6 Överföring av domännamn till en ny användare	9
1.6.1 Rätt att framställa en begäran om överföring.....	9
1.6.2 Överföringstid	9
1.7 Byte av förmedlare	9
1.7.1 Problemsituationer.....	10
1.8 När förmedlingsverksamheten upphör	10
1.8.1 Information om Traficom förbudsbeslut	10
1.8.2 Avslutande av förskottskontot.....	10
1.9 Anmälan som förmedlare	10
1.9.1 Återförsäljarnas förmedlingsverksamhet.....	11
2 Informationssäkerheten i förmedlingsverksamheten	12
2.1 Informationssäkerhet i praktiken.....	12
2.1.1 Informationssäkerhetens delområden	12
2.2 Riskhantering	13
Riskhanteringens mål	14
Identifiering och hantering av risker	14
2.3 Informationsmaterial.....	14
2.3.1 Klassificering av material.....	14
2.3.2 Dokument om informationsmaterial.....	15
2.4 Övervakning av informationssäkerheten.....	15
2.4.1 Upptäckt av hot	15
2.4.2 Förebyggande av hot	15
2.4.3 Dokumentation av övervakningen.....	15
2.5 Hantering av hot- och störningssituationer	15
2.6 Ändringshantering	16
2.6.1 Planering av ändringsarbeten.....	16
2.6.2 Dokumentation av ändringsarbeten	16
2.7 Säkerhetskopiering	16
2.8 Dataskyddet i förmedlingsverksamheten	17

2.8.1	Personuppgifter som ska anmälas till registret	17
2.8.2	Syftet med och varaktigheten av behandlingen av personuppgifter	18
2.8.3	Rättigheterna för användaren av domännamnet.....	18
2.8.4	Återförsäljare och underleverantörer.....	18
2.9	Anmälningsskyldighet vid informationssäkerhetsstörningar	19
2.9.1	Tidtabell för anmälan	19
2.9.2	Betydande kränkningar av informationssäkerheten	19
	Typer av kränkningar av informationssäkerheten som omfattas av anmälningsskyldigheten	19
2.10	Namnserverar	20
2.10.1	Rekommendationer	20
2.10.2	Krav och rekommendationer för SOA-posten	21
2.10.3	DNSSEC - säkerhetstillägg för namntjänsten	21
2.10.4	Namnservertest	21
2.11	Tekniska gränssnitt.....	22
2.11.1	Webbanvändargränssnitt	22
2.11.2	EPP-gränssnitt	22
2.11.3	RFC-standarder som EPP bygger på	22
2.11.4	KATAKRI-krav vid användning av EPP-gränssnittet	23
2.11.5	Övriga tekniska tjänster.....	23
Bilaga A: Snabbguide för nya förmedlare - checklista		24
1.	Lagstadgade förutsättningar	24
2.	Tekniska krav	24
3.	Administrativa förberedelser	24
4.	Anmälan till Traficom	24
Bilaga B: Kontaktuppgifter		26
	Transport- och kommunikationsverket Traficom	26
	Övriga myndigheter och register	26
Bilaga C: Terminologi		27

Inledning

Denna guide är avsedd för alla som överväger eller redan håller på att anmäla sig som förmedlare av fi-domännamn till Transport- och kommunikationsverket Traficom. Guiden lämpar sig också för befintliga förmedlare som vill repetera sina skyldigheter och krav. Guiden behandlar inte DNS-tjänsteleverantörernas skyldigheter.

Guiden omfattar två centrala helheter:

- Kapitel 1 - Domännamnsförmedlarens uppgifter och skyldigheter: beskriver förmedlarens lagstadgade serviceskyldigheter gentemot kunderna, såsom registrering, uppdatering av uppgifter, förnyelse, uppsägning och byte av förmedlare.
- Kapitel 2 - Informationssäkerheten i förmedlingsverksamheten: behandlar krav som gäller hanteringen av informationssäkerheten, riskhantering, dataskydd, namnservrar och tekniska gränssnitt.

Guidens innehåll grundar sig på lagen om tjänster inom elektronisk kommunikation (917/2014) samt Traficoms domännamnsföreskrift 68. Guiden har senast uppdaterats i juni 2026 (version 2.0).

1 Domännamnsförmedlarens uppgifter och skyldigheter

En domännamnsförmedlare hjälper och ger sina kunder råd i frågor som gäller fi-domännamn. Förmedlaren registrerar fi-domännamnen och gör de ändringar i dem som kunderna begär.

Användaren av ett domännamn sköter alla ärenden som gäller fi-domännamn med sin egen förmedlare. Med stöd av lagen om tjänster inom elektronisk kommunikation (917/2014) är förmedlaren skyldig att se till att användarens rättigheter tillgodoses.

På sina kunders begäran sköter förmedlarna i fråga om ett fi-domännamn:

- registrering i Traficom domännamnsregister
- uppdatering av uppgifter
- förnyelse av giltighetstiden
- byte från en förmedlare till en annan
- överföring från en användare till en annan
- uppsägning.

Förmedlaren är dessutom skyldig att ge sina kunder:

- allmän rådgivning om fi-domännamn
- information om förmedlingsverksamheten har upphört eller om Traficom har meddelat ett förbudsbeslut som gäller förmedlaren.

1.1 Domännamnsförmedlarens serviceskyldigheter och priser

1.1.1 Betalning för registrering och förnyelse

Förmedlaren betalar Traficom för registreringar och förnyelser av kundernas domännamn via förmedlarens tekniska gränssnitt. Registreringarna och förnyelserna dras av från förmedlarens förskottskonto. Priserna bestäms enligt giltighetstiden:

Giltighetstid	Pris (inkl. moms 0 %)
1 år	12 €
2 år	24 €
3 år	36 €
4 år	48 €
5 år	60 €

⚠ Avgifterna återbetalas inte

Traficom återbetalar inte avgiften till förmedlaren, även om domännamnet av misstag har registrerats felaktigt eller om Traficom senare genom beslut avför domännamnet ur registret.

1.2 Skyldighet att ge kunderna råd

Domännamnsförmedlaren ska ge sina kunder råd innan fi-domännamn registreras. Rådgivning ska ges åtminstone om domännamnets form, innehåll och lagenlighet.

Informationen ska vara tillgänglig för såväl nuvarande som framtida användare av domännamn, oberoende av om kunderna redan har ingått ett avtalsförhållande med förmedlaren eller inte. Det slutliga ansvaret för domännamnets lagenlighet ligger hos användaren av domännamnet.

Dessutom ska domännamnsförmedlaren tydligt informera om hur och var kunden vid behov kan få nyckeln för byte av förmedlare eller nyckeln för överföring av domännamnet. Det räcker att kunden får rådgivning efter att kunden har ingått ett avtalsförhållande med sin förmedlare.

1.2.1 Minimikrav på rådgivningen

Förmedlaren får fritt välja på vilket sätt informationsskyldigheten fullgörs, men till sitt innehåll ska domännamnsförmedlaren erbjuda sina kunder åtminstone följande information om domännamnets innehåll och form:

Skyddade namn och varumärken

Enligt lagen om tjänster inom elektronisk kommunikation är skyddade namn och märken:

- namn eller märken som antecknats i Finlands handels-, varumärkes-, förenings-, stiftelse- eller partiregister
- namn på offentliga samfund, statliga affärsverk, självständiga offentligrättsliga inrättningar, offentligrättsliga föreningar och främmande staters beskickningar
- inarbetade namn, sekundära kännetecken eller varumärken som avses i firmalagen och varumärkeslagen
- EU-varumärken som antecknats i EUIPO:s varumärkesregister
- produkter med skyddade beteckningar enligt livsmedelslagen samt beteckningar som avses i lagen om geografiska beteckningar för hantverks- och industriprodukter

Förmedlaren ska erbjuda sina kunder länkar till följande register:

- Patent- och registerstyrelsen (PRS): företags- och organisationsdatasystemet, föreningsregistret, varumärkesregistret - prh.fi
- Europeiska unionens immaterialrättsmyndighet (EUIPO): registret över EU-varumärken - euipo.europa.eu
- Europeiska unionens register över geografiska beteckningar: eAmbrosia - ec.europa.eu/agriculture/eambrosia/geographical-indications-register

Domännamnets lagenlighet

Ett domännamn får vid tidpunkten för registreringen inte:

- motsvara någon annans skyddade namn eller märke, om inte användaren av domännamnet kan ange en godtagbar grund för registreringen
- likna någon annans skyddade namn eller märke, om domännamnet registreras i uppenbart vinnings- eller skadesyfte.

Tillåtna tecken i ett domännamn

Tillåtna tecken är bokstäverna a–z, siffrorna 0–9, de nationella tecknen å, ä och ö, tecknen i de samiska språk som talas i Finland samt bindestreck-minustecknet.

Nationella tecken och ACE-format (Punycode)

Domännamn som innehåller nationella tecken visas i domännamnsystemet i ACE-format (ASCII Compatible Encoding, Punycode).

Exempel: ääkkönen.fi → xn--kknen-fraa0m.fi

Kunderna ska informeras om de tekniska begränsningarna för domännamn som innehåller nationella tecken, och vid behov rekommenderas att de ansöker om både ett domännamn med nationella tecken och ett motsvarande namn utan sådana tecken (till exempel ääkkönen.fi och aakkonen.fi).

Konverteringsverktyg finns bland annat på Traficoms webbplats .

Anvisningar för att få nycklarna

Domännamnsförmedlaren ska alltid erbjuda sina kunder möjlighet att skriftligen begära nyckeln för byte av förmedlare eller nyckeln för överföring av domännamnet. Domännamnsförmedlaren kan till exempel på sin webbplats ge anvisningar om förutsättningarna och förfarandena för att få nyckeln.

1.3 Att se till att uppgifterna är korrekta och aktuella

Förmedlaren håller sina kunders uppgifter uppdaterade i fi-domännamnsregistret både vid registreringstidpunkten och senare när uppgifterna ändras. Förmedlaren ska identifiera sina kunder. Förmedlaren ska göra de verksamhetsprinciper och förfaranden offentligt tillgängliga genom vilka den säkerställer att de användaruppgifter som antecknats i domännamnsregistret är korrekta och aktuella.

⚠ Kritisk skyldighet: anteckning av användaren

Ett fi-domännamn ska alltid registreras i den faktiska användarens namn. Domännamnet får inte antecknas i en integritets- eller proxytjänstleverantörs namn. Förmedlaren får inte anteckna kundens domännamn i sitt eget namn. En felaktig anteckning av användaren kan i värsta fall leda till skadeståndsansvar.

När kunden framställer en begäran är förmedlaren skyldig att genomföra följande ändringar:

- uppdatering av kontaktuppgifterna för användaren av domännamnet
- uppsägning av domännamnet
- överföring av domännamnet till en annan användare
- byte av förmedlare för domännamnet
- förnyelse av domännamnet.

1.3.1 Uppdatering av kontaktuppgifter

Förmedlaren ska hålla sina fi-domännamnskunders uppgifter uppdaterade både på kundens begäran och på eget initiativ. Om kunden orsakas skada på grund av förmedlarens försummelse kan kunden kräva skadestånd.

1.3.2 Lagstadgad processadress

Traficom använder den e-postadress som antecknats i domännamnsregistret (processadressen) för höranden och delgivningar. En handling eller ett beslut som har sänts till adressen anses ha delgetts den tredje dagen efter att meddelandet sändes. Förmedlaren ska säkerställa att processadressen fungerar tekniskt.

Processadressens betydelse

Det är obligatoriskt att meddela Traficom en processadress både för förmedlaren själv och för varje kunds domännamn.

Förmedlaren ansvarar för att meddela adressen och hålla den uppdaterad.

Dessutom kan andra e-postadresser meddelas i systemet, till exempel för teknisk kommunikation.

1.4 Förnyelse av domännamn

Ett domännamn som antecknats i domännamnsregistret är giltigt i minst ett år och högst fem år. Förmedlaren kan förnya anteckningen för ett, två, tre, fyra eller fem år i taget.

1.4.1 Förmedlarens skyldigheter när giltighetstiden löper ut

När giltighetstiden för ett fi-domännamn håller på att löpa ut ska domännamnsförmedlaren:

- informera användaren i god tid om att giltighetstiden löper ut
- ge användaren anvisningar om hur en begäran om förnyelse görs
- redogöra för användaren vilka följderna blir om domännamnet inte förnyas.

Förmedlaren och kunden kan avtala om automatisk förnyelse. Det hör inte till Traficom behörighet att övervaka avtal mellan förmedlaren och användaren eller att avgöra avtalstvister.

1.5 Uppsägning av domännamn

Användaren av ett fi-domännamn kan om så önskas säga upp sitt domännamn innan giltighetstiden löper ut. Förmedlaren avför på begäran domännamnet ur Traficoms register.

Domännamnsförmedlaren ansvarar för att:

- domännamnet sägs upp endast på begäran av användaren av domännamnet eller av ett ombud som denne har befullmäktigat
- ingen utomstående part avsiktligt eller oavsiktligt säger upp domännamn
- det, när användaren av domännamnet är en organisation, säkerställs att den som säger upp domännamnet har rätt att göra det (till exempel firmateckningsrätt som antecknats i handelsregistret).

⚠ Problemsituationer vid uppsägning

En felaktig uppsägning av ett domännamn kan ha betydande ekonomiska konsekvenser. Förmedlaren kan i värsta fall bli skadeståndsskyldig för en felaktig uppsägning.

Avtals-, skadestånds- eller konsumenträttsliga frågor som föranleds av uppsägningen avgörs med stöd av annan lagstiftning.

1.6 Överföring av domännamn till en ny användare

Användaren av ett domännamn kan om så önskas överföra sitt giltiga domännamn till en annan användare. När domännamnsförmedlaren har tagit emot en begäran om överföring:

- säkerställer förmedlaren att den som framställer begäran har rätt att överföra domännamnet
- sänder förmedlaren domännamnets överföringsnyckel till användaren av domännamnet utan att se nyckelkodens innehåll
- överför förmedlaren domännamnet från en användare till en annan inom fem vardagar efter att överföringsnyckeln har lämnats till förmedlaren.

Överföringsnyckel

Överföringsnyckeln är en kod som fastställs av Traficom och som förmedlaren varken ser eller bestämmer.

Nyckeln sänds alltid till domännamnets nuvarande användare, som själv ska ge den till förmedlaren för överföringen.

Användaren kan befullmäktiga antingen sin egen förmedlare eller mottagarens förmedlare att utföra överföringen. Den sistnämnda behöver utöver överföringsnyckeln även nyckeln för byte av förmedlare.

1.6.1 Rätt att framställa en begäran om överföring

Domännamnsförmedlaren ska säkerställa att ingen annan än användaren av domännamnet eller ett ombud som denne har befullmäktigat begär överföringen. Om begäran framställs av någon annan part ska den som framställer begäran visa tillräcklig fullmakt.

1.6.2 Överföringstid

Domännamnsförmedlaren ska genomföra överföringen tekniskt inom fem vardagar från det att den tidigare användaren har lämnat överföringsnyckeln och den nya användarens uppgifter till förmedlaren. Tidsfristen är ett servicenivåkrav som grundar sig på Traficom föreskrift.

1.7 Byte av förmedlare

Användaren av ett domännamn kan fritt byta domännamnsförmedlare. Byte av förmedlare kräver ingen särskild orsak.

Stegen vid bytet

1. Användaren befullmäktigar antingen den nya förmedlaren att skaffa nyckeln för byte av förmedlare från den tidigare förmedlaren, eller begär själv nyckeln av den tidigare förmedlaren och lämnar den till den nya förmedlaren. Begäran ska göras skriftligen.
2. Den tidigare förmedlaren lämnar nyckeln för byte av förmedlare inom fem vardagar från en berättigad begäran, efter att ha säkerställt att den som begär nyckeln har rätt till den.
3. Den nya förmedlaren får bytesnyckeln och tar över administrationen av domännamnet.

Nyckel för byte av förmedlare

En kod med vars hjälp administrationen av ett domännamn överförs från en förmedlare till en annan.

Den tidigare förmedlaren skapar nyckeln i domännamnsystemet och lämnar den på valfritt sätt (till exempel per e-post eller telefon) till den som på berättigade grunder begär den.

1.7.1 Problemsituationer

Om den tidigare förmedlaren trots upprepade begäranden inte lämnar bytesnyckeln till den nya förmedlaren eller användaren inom utsatt tid, kan den nya förmedlaren be Traficom att lämna bytesnyckeln till användaren.

1.8 När förmedlingsverksamheten upphör

Om en domännamnsförmedlare upphör med sin verksamhet ska detta meddelas Traficom och förmedlarens egna kunder senast två veckor på förhand. Detta ger kunderna möjlighet att hålla sina domännamn funktionsdugliga och byta administratör för namnservrarna innan verksamheten upphör.

Meddelandena ska göras kundspecifikt. Det räcker inte med att enbart informera på webbplatsen. E-post är ett effektivt sätt, men det är bra att försöka nå kunderna även per telefon.

1.8.1 Information om Traficom förbudsbeslut

Traficom övervakar att domännamnsförmedlingsverksamheten är lagenlig och kan meddela förmedlaren ett beslut om förbud mot att bedriva verksamhet, om förmedlaren trots anmärkningar inte åtgärdar sin försummelse.

Om Traficom meddelar ett förbudsbeslut ska förmedlaren utan dröjsmål informera sina egna kunder om detta, så att de vid behov kan skaffa en ny förmedlare.

Traficom verkställer förbudsbeslutet genom att stänga förmedlarens tekniska gränssnitt, antingen så att förmedlaren inte längre kan registrera nya domännamn eller så att förmedlaren dessutom inte ens kan administrera befintliga domännamn.

1.8.2 Avslutande av förskottskontot

En förmedlare som har upphört med sin förmedlingsverksamhet kan be Traficom återbetala de oanvända medel som förmedlaren har satt in på förskottskontot.

1.9 Anmälan som förmedlare

Den som planerar att bli förmedlare av fi-domännamn ska innan anmälan görs till Traficom noggrant sätta sig in i alla krav som föreskrivs i 21 kap. i lagen om tjänster inom elektronisk kommunikation.

Anmälan som förmedlare görs på Traficom elektroniska blankett. Innan anmälan godkänns kontrollerar Traficom att förmedlaren har fyllt i det självvärderingsverktyg som Traficom har fastställt och med vilket förmedlaren kan visa att informationssäkerhetsskyldigheterna iakttas.

Ändringar i förmedlarens uppgifter ska utan dröjsmål meddelas Traficom. Traficom rekommenderar att uppdateringarna görs inom tre dagar från ändringen.

Förmedlaren får använda fi-förmedlarlogotypen i förmedlingsverksamheten för fi-domännamn. Versioner av logotypen som lämpar sig för publicering finns på Traficoms webbplats .

1.9.1 Återförsäljarnas förmedlingsverksamhet

Om förmedlaren anlitar återförsäljare i förmedlingsverksamheten för fi-domännamn ansvarar förmedlaren även för deras verksamhet. Förmedlaren ska anteckna uppgifterna om återförsäljaren i fi-domännamnsregistret och hålla dem uppdaterade. Förmedlaren ska i uppgifterna för varje domännamn anteckna om en återförsäljare anlitas för administrationen av domännamnet i fråga.

2 Informationssäkerheten i förmedlingsverksamheten

Förmedlaren ska sörja för informationssäkerheten genom att förbereda sig på hot och ingripa vid avvikelser. Minimikraven på informationssäkerheten tryggar både förmedlingsverksamheten och rättigheterna för användaren av domännamnet.

Med informationssäkerhet avses enligt 3 § 28 punkten i lagen om tjänster inom elektronisk kommunikation administrativa och tekniska åtgärder genom vilka informationens konfidentialitet, integritet och tillgänglighet säkerställs.

Förmedlaren ska fylla i det självutvärderingsverktyg för informationssäkerhet som Traficom har fastställt.

Dokumentationsskyldighet

Beredskapsplanen ska dokumenteras.

Transport- och kommunikationsverkets domännamnsföreskrift 68 beskriver minimikraven på hanteringen av informationssäkerheten, vilka förmedlaren ska genomföra i sin verksamhet.

Utifrån dokumentationen kan Traficom vid behov verifiera att förmedlaren iakttar informationssäkerhetsskyldigheterna.

2.1 Informationssäkerhet i praktiken

Domännamnsförmedlaren ska dokumentera och upprätthålla en aktuell beskrivning av hur den i sin verksamhet beaktar informationssäkerhetens olika delområden. Traficom specificerar inte separat vilka dokument som krävs - helheten avgörs enligt förmedlarens egen prövning.

2.1.1 Informationssäkerhetens delområden

Förmedlaren ska beakta följande delområden:

Administrativ informationssäkerhet

- styrdokument för informationssäkerheten (vanligtvis informationssäkerhetspolicy och -arkitektur)
- processer och hanteringen av dem
- riskhantering och tryggnad av kontinuiteten
- dokumentationspraxis och -system
- auditerings- och övningsförfaranden.

Personalsäkerhet

- personernas informationssäkerhetsansvar och skyldigheter
- personalens informationssäkerhetskompetens och utvecklingen av den
- bakgrundskontroller av personer
- nyckelpersonsrisker
- förhindrande av farliga kombinationer av ansvar och arbetsuppgifter samt arbetsrotation
- förfarande som iakttas när en anställning upphör.

Utrustnings-, programvaru- och datakommunikationssäkerhet

- hantering av sårbarheter
- upptäckt av kränkningar av informationssäkerheten
- ändringshantering.

Informationsmaterial- och driftssäkerhet

- säkerställande av informationens konfidentialitet, integritet och tillgänglighet
- klassificering av informationsmaterial och hantering enligt klassificeringen
- ansvaret för att upprätthålla registret över åtkomsträttigheter: tilldelning, ändring och borttagning av rättigheter
- förhindrande av att åtkomsträttigheter ackumuleras
- förhindrande av obehörig åtkomst till administrations- och konfigurationsuppgifter samt till kund-, debiterings- och logguppgifter
- förvaring och förstöring av informationsmaterial.

Fysisk säkerhet

- lokalernas läge och omgivningens säkerhet
- tillträdeskontroll
- strukturellt skydd.

Vid behov har Traficom rätt att auditera domännamnsförmedlarens förmedlingsverksamhet.

2.2 Riskhantering

Domännamnsförmedlaren ska identifiera de funktioner, uppgifter och system som är viktiga för kontinuiteten i förmedlingsverksamheten samt regelbundet bedöma och hantera de informationssäkerhetsrisker som riktas mot dem. Riskhanteringsprocesser och resultat ska dokumenteras.

Informationssäkerhetsrisker kan orsakas till exempel av:

- mänskliga fel
- brister i de anvisningar som getts personalen eller underlåtenhet att följa dem
- stölder eller skadegörelse
- fel och funktionsstörningar i utrustning, system eller programvara
- spridning av skadliga program
- att informationsmaterial förstörs
- brand eller vattenskada
- fel och försummelser hos en underleverantör eller en aktör som hör till partnernätverket.

Riskhanteringsens mål

Målet med riskhanteringen är bland annat att:

- påskynda återhämtningen från informationssäkerhetsproblem
- minska kostnader och skador som orsakats av informationssäkerhetsproblem
- rikta investeringar som förbättrar informationssäkerheten
- förbättra förmedlingsverksamhetens kvalitet och produktivitet
- optimera riskhanteringen ekonomiskt och förebygga att riskerna realiserats.

Identifiering och hantering av risker

Traficom ställer inget krav på att en viss standard ska följas. Lämpliga referensramar är till exempel ISO/IEC 27005, NIST 800-30 och OCTAVE. Riskhanteringen ska ha tydligt fördelat ansvar och en fastställd tidsplan.

Riskbedömning görs vanligtvis:

- regelbundet varje år
- när nya tjänster eller funktioner definieras
- efter att en eventuell risk har realiserats.

2.3 Informationsmaterial

Domännamnsförmedlaren ska ha ett klassificeringssystem för informationsmaterial som är viktigt för förmedlingsverksamheten samt ett tillhörande hanteringsförfarande. En aktuell dokumentation av klassificeringskriterierna och hanteringsförfarandena ska upprättas.

2.3.1 Klassificering av material

Förmedlaren ska fastställa klassificeringskriterier som lämpar sig för den egna verksamheten. Exempel på klassificering:

- offentligt
- konfidentiellt

- hemligt.

2.3.2 Dokument om informationsmaterial

I dokumentationen ska bland annat följande beaktas: hanterings- och ändringsrättigheter, förvaring och kryptering, utskrift och kopiering, säkerhetskopiering, mottagande, delning, sändning och transport samt arkivering och förstöring av material.

2.4 Övervakning av informationssäkerheten

Domännamnsförmedlaren ska kontinuerligt övervaka sin förmedlingsverksamhet. Med hjälp av övervakningen kan situationer som stör eller hotar verksamheten upptäckas eller helt förebyggas.

2.4.1 Upptäckt av hot

Övervakningen ska ske med en hanteringsmekanism som lämpar sig för förmedlingsverksamheten och som så snabbt som möjligt upptäcker problem som stör informationssäkerhetsläget. Exempel på situationer som ska upptäckas:

- överbelastningsattacker
- dataläckor
- försök till dataintrång
- alltför omfattande användarrättigheter.

2.4.2 Förebyggande av hot

Övervakningsmekanismer kan till exempel vara:

- programvarularm och kvalitetsmätare för tjänsten som indikerar avvikelser från den normala verksamheten
- meddelanden om upptäckta sårbarheter i utrustning eller programvara som förebådar informationssäkerhetsproblem.

2.4.3 Dokumentation av övervakningen

Aktuell dokumentation av förmedlingsverksamhetens övervakningsmekanismer ska upprättas och upprätthållas, så att förmedlaren vid behov kan visa med vilka medel den uppfyller de ställda kraven.

2.5 Hantering av hot- och störningssituationer

Domännamnsförmedlaren ska på förhand utarbeta tydliga förfarandeanvisningar för att reda ut situationer som stör eller hotar informationssäkerheten i förmedlingsverksamheten. Med hjälp av anvisningarna minimeras situationernas konsekvenser och återhämtningen sker utan ogrundat dröjsmål.

Förfarandeanvisningarna ska fastställa:

- hur hanteringen av informationssäkerheten organiseras

- vilka aktörer som har ansvar för informationssäkerheten
- hur de ansvariga personerna kan nås.

Anvisningarnas viktigaste mål är att skapa beredskap att så snabbt som möjligt reda ut vad som orsakat ett informationssäkerhetsproblem och att minimera händelsens konsekvenser. I anvisningarna ska även särskilda anvisningar om korrigerande åtgärder vid betydande störningssituationer beaktas, såsom jourarrangemang.

2.6 Ändringshantering

Domännamnsförmedlaren ska organisera ändringar, underhåll och uppdateringar så att de orsakar så lite störningar som möjligt i förmedlingsverksamheten.

Förmedlaren ska genomföra ändringar i nät, programvara, utrustning, konfigurationer, gränssnitt och utrustningsutrymmen på ett kontrollerat och planmässigt sätt.

2.6.1 Planering av ändringsarbeten

För att hantera en ändringssituation ska förmedlaren omsorgsfullt på förhand:

- planera hur ändringsarbetet ska framskrida
- beräkna de resurser som behövs
- bedöma ändringsarbetets konsekvenser och varaktighet
- planera sina fortsatta åtgärder, ifall ändringsarbetet inte lyckas som planerat.

Till exempel vid byte av programvara i utrustning är det bra att i mån av möjlighet simulera ändringens effekter på förhand, så att fel kan lokaliseras och korrigeras i förväg.

2.6.2 Dokumentation av ändringsarbeten

Förmedlaren ska på förhand fastställa och dokumentera de processer och den praxis som hänför sig till ändringsarbeten, så att planmässighet och förutsägbarhet iakttas i alla ändringsarbeten.

2.7 Säkerhetskopiering

Domännamnsförmedlaren ska ha en dokumenterad säkerhetskopieringspraxis för uppgifter och system som är kritiska för förmedlingsverksamheten. I praktiken ska förmedlaren bedöma vilka uppgifter, system och inställningar som är nödvändiga för kontinuiteten i förmedlingsverksamheten och säkerställa att de kan återställas i en störnings- eller krissituation.

I säkerhetskopieringspraxisen rekommenderas att åtminstone följande beskrivs:

- Vilka uppgifter och system som säkerhetskopieras
- Hur ofta säkerhetskopior tas

- Hur länge säkerhetskopiorna förvaras
- Hur säkerhetskopiorna skyddas mot obehörig användning, ändring och förstörelse
- Vem som ansvarar för säkerhetskopieringen och återställningen
- Hur och hur ofta återställningen testas.

Säkerhetskopieringen ska omfatta material som är kritiskt för förmedlarens egen verksamhet, såsom kund- och avtalsuppgifter, uppgifter som hänför sig till administrationen av domännamn, systeminställningar som är väsentliga för förmedlingsverksamheten samt andra sådana uppgifter vars förlust skulle kunna förhindra eller väsentligt störa förmedlingsverksamheten för fi-domännamn.

Förmedlaren ska beakta att säkerhetskopiornas skyddsnivå ska motsvara konfidentialiteten och kriticiteten hos den information som säkerhetskopieras. Återställningsförmågan ska testas regelbundet, eftersom enbart förekomsten av en säkerhetskopia ännu inte säkerställer att informationen kan återställas vid behov.

2.8 Dataskyddet i förmedlingsverksamheten

Förmedlare av fi-domännamn samlar in och behandlar personuppgifter om användarna av fi-domännamn för att registrera fi-domännamn. Bestämmelser om behandling av personuppgifter finns i EU:s allmänna dataskyddsförordning (679/2016, GDPR) och i dataskyddslagen (1050/2018). Bestämmelser om utlämnande av uppgifter finns i 170 § 1 mom. 10 punkten i lagen om tjänster inom elektronisk kommunikation (917/2014).

I fråga om de uppgifter som antecknats i domännamnsregistret är Traficom personuppgiftsansvarig, och förmedlarna är personuppgiftsbiträden för Traficom räkning. När domännamnsförmedlaren behandlar personuppgifter om användarna av domännamn i sin förmedlingsverksamhet ska den iakttä de skyldigheter som föreskrivs för personuppgiftsbiträden i artikel 28 i GDPR.

Förmedlaren av fi-domännamn är dock en självständig personuppgiftsansvarig enligt dataskyddsförordningen i fråga om de personuppgifter om användarna av fi-domännamn som förmedlaren behandlar i sin förmedlingsverksamhet och som inte krävs att antecknas i domännamnsregistret.

2.8.1 Personuppgifter som ska anmälas till registret

I förmedlingsverksamheten samlas med stöd av lagen och föreskriften följande personuppgifter in om användaren av domännamnet:

- namn
- personbeteckning eller någon annan identifierande beteckning
- postadress
- telefonnummer
- e-postadress (processadress).

⚠ Förmedlare som är etablerade utanför EU/EES-området

Förmedlare av fi-domännamn som är etablerade utanför EU/EES-området kan inte registrera fi-domännamn för privatpersoner, om etableringslandet inte omfattas av ett av EU godkänt och giltigt arrangemang för dataöverföring.

Begränsningen gäller även förmedlare i Förenta staterna som inte är certifierade enligt det gällande dataskyddsramverket

2.8.2 Syftet med och varaktigheten av behandlingen av personuppgifter

Förmedlaren får behandla de personuppgifter som den har antecknat i fi-domännamnsregistret endast under den tid som fi-domännamnet administreras av förmedlaren i fråga och/eller domännamnet är giltigt, inklusive skyddstider.

Förmedlaren ansvarar för att den raderar personuppgifterna om användarna av fi-domännamn ur sina egna system när grunden för behandlingen av uppgifterna, dvs. förmedlingsverksamheten för domännamnet, upphör.

Om förmedlaren erbjuder andra tjänster (till exempel webbplats- eller e-posttjänster) ska förmedlaren ha någon annan behandlingsgrund enligt GDPR för dessa tjänster.

2.8.3 Rättigheterna för användaren av domännamnet

Användaren av ett domännamn har rätt:

- att veta vilka parter som behandlar personuppgifterna - användarens uppgifter behandlas åtminstone av förmedlaren och Traficom
- att veta för vilket ändamål uppgifterna används - för registrering och administration av domännamnet samt för tvistlösning
- att granska och rätta felaktiga uppgifter
- att begränsa behandlingen av personuppgifter i situationer enligt artikel 18 i GDPR
- att lämna in klagomål till dataombudsmannen (tietosuoja.fi).

2.8.4 Återförsäljare och underleverantörer

Återförsäljarna fungerar som personuppgiftsbiträden för förmedlarens räkning. Förmedlaren ansvarar för att dess återförsäljare förbinder sig till personuppgiftsbiträdets skyldigheter enligt artikel 28 i GDPR. Förmedlaren ansvarar fullt ut för sina underleverantörers verksamhet.

2.9 Anmälningsskyldighet vid informationssäkerhetsstörningar

Förmedlaren ska utan dröjsmål meddela Traficom om dess förmedlingsverksamhet för domännamn utsätts för en betydande kränkning av informationssäkerheten, för ett hot om en betydande kränkning av informationssäkerheten eller för en händelse som förhindrar eller väsentligt stör verksamheten.

Anmälan innehåll

I anmälan ska följande redogöras: störningens eller hotets uppskattade varaktighet, konsekvenserna, de korrigerande åtgärderna, åtgärderna för att förhindra att störningen upprepas samt i mån av möjlighet störningens orsak.

Anmälan görs i första hand på en elektronisk blankett:

Blankett för anmälan om informationssäkerhetsincident

I allvarliga situationer eller för att utreda obehöriga ändringar tas kontakt även per telefon till det nummer som har meddelats förmedlarna.

2.9.1 Tidtabell för anmälan

En störningsanmälan ska göras inom 24 timmar från det att störningssituationen har kommit till förmedlarens kännedom. Om alla uppgifter inte är tillgängliga görs en preliminär anmälan inom 24 timmar, och den kompletteras senast tre (3) dagar efter den preliminära anmälan.

2.9.2 Betydande kränkningar av informationssäkerheten

Som betydande kan betraktas en störning som riktas mot:

- domännamnsförmedlarens egna tjänster och produktionssystem
- informationssäkerheten, skyddet av personuppgifter eller företagshemligheter hos domännamnsförmedlarens kunder
- den finska fi-rot som administreras av Traficom (direkt eller indirekt).

Som betydande kan också betraktas verksamhet som upprepas ofta, är exceptionellt långvarig eller förefaller avsiktlig, samt en störning som inte kan avhjälpas enbart genom förmedlarens egna åtgärder.

Typer av kränkningar av informationssäkerheten som omfattas av anmälningsskyldigheten

Betydande informationssäkerhetsstörningar som ska anmälas är bland annat:

- dataintrång i domännamnsförmedlarens informationssystem
- obehörig åtkomst till förmedlarens system
- en sårbarhet eller ett konfigurationsfel som äventyrar informationssäkerheten i förmedlarens system
- att inloggningsuppgifter kommer till en tredje parts kännedom
- att koder som används för Traficoms system hamnar hos utomstående
- möjlighet att obehörigt ändra uppgifter om domännamn som förmedlaren administrerar

- obehöriga ändringar i Traficom domännamnsregister som görs av förmedlarens egen personal
- överbelastningsattacker som lamslår förmedlarens system eller påverkar funktionen hos Traficom system.

Traficom rekommenderar att förmedlarna enligt egen prövning även anmäler kränkningar av informationssäkerheten och hot om sådana som är mindre än betydande - dessa uppgifter kan ha betydelse för skötseln av Traficom övriga informationssäkerhetsuppgifter.

2.10 Namnservrar

Domännamnsförmedlaren ansvarar för att de namntjänster som är kopplade till de fi-domännamn som erbjuds kunderna har definierats i enlighet med de tekniska kraven.

Ett fi-domännamn kan registreras antingen med fungerande namnservrar eller helt utan namnservrar. Om namnservrar dock anges ska alla fungera. Om användaren vill behålla domännamnet i sitt namn utan funktioner (s.k. parkeringstjänst) ska namnservrarna tas bort ur fi-roten.

Krav på namnservrarna

Ett domännamn ska definieras för minst två och högst tio av varandra oberoende namnservrar (Traficom föreskrift 68). Namnservrarna är oberoende av varandra när de fungerar:

- på olika serverutrustning
- på olika IP-adresser
- bakom olika internet-förbindelser.

Alla namnservrar ska dessutom vara anslutna till internet, och deras konfiguration ska kunna kontrolleras genom namntjänstförfrågningar som Traficom utför.

Traficom kontrollerar regelbundet att alla namnservrar fungerar. Vid felaktiga konfigurationer sänds en anmärkning per e-post till förmedlaren eller till den adress som namnservrarnas administratör har meddelat.

2.10.1 Rekommendationer

Traficom rekommenderar att:

- zonöverföring (AXFR/DNS zone transfer) förhindras för obehöriga
- namnservrarna inte returnerar korrekt information vid förfrågningar om programvaruversioner (för att undvika en informationssäkerhetsrisk).

2.10.2 Krav och rekommendationer för SOA-posten

I SOA-postens (Start of Authority) MNAME-fält ska den primära namnserverns namn anges. I RNAME-fältet ska det finnas en fungerande e-postadress till administratören (utan @-tecken, som ersätts med en punkt, till exempel hostmaster.domain.fi).

Parameter	Rekommenderat värde	Förklaring
Refresh	86400 (24 h)	Hur ofta de sekundära namnserverna kontrollerar ändringar
Retry	7200 (2 h)	Intervallet mellan nya försök efter en misslyckad hämtning
Expire	3600000 (~1000 h)	Hur länge en gammal zonfil bevaras
Minimum TTL	172800 (2 dygn)	Standardlivslängd för resursposter (resource records, RR)
Serienummer	YYYYMMDDnn	Datumbaserat, ökar vid varje uppdatering

Det rekommenderade formatet för serienumret är YYYYMMDDnn. Serienumret får inte vara noll (0), och dess värde ska öka med ett vid varje uppdatering.

2.10.3 DNSSEC - säkerhetstillägg för namntjänsten

DNSSEC (Domain Name System Security Extensions) är en tjänst som förbättrar namntjänstens informationssäkerhet och med vars hjälp man kan säkerställa att den information som fås från namnservern har ett tillförlitligt ursprung och är oförändrad. DNSSEC kan tas i bruk även för fi-domännamn.

När DNSSEC används signeras svaren på namntjänstförfrågningar elektroniskt, varvid besökarna på en webbplats kan försäkra sig om att de styrs till rätt sida.

Ibruktagande av DNSSEC och DS-poster

Förmedlaren kan ta i bruk DNSSEC-tjänsten genom att signera domännamnets uppgifter och lägga till DS-posterna via EPP-gränssnittet eller webbanvändargränssnittet.

Nyckelbyten kan automatiseras med hjälp av EPP-gränssnittet.

Fi-zonens offentliga nycklar publiceras i rotzonen. Tillitsankaret finns på IANA:s DNSSEC-sidor (iana.org/dnssec).

Mer information: fi-domain-tech@traficom.fi

2.10.4 Namnservertest

Med namnservertestet på Traficoms webbplats kan man kontrollera om ett fi-domännamn har definierats enligt kraven, om namntjänsterna fungerar och om DNSSEC används. Testet kan användas även innan domännamnet registreras och i samband med namnserverändringar.

Namnservertest

Zonemaster.fi kontrollerar att domännamnets namntjänster fungerar tekniskt och att inställningarna är korrekta. Det testas till exempel delegering, namnserversvar, DNSSEC, nåbarhet och allmänna konfigurationsfel, rapporterar upptäckta brister och varningar samt ger rekommendationer för att förbättra namntjänsterna.

Mer information: <https://zonemaster.fi>

2.11 Tekniska gränssnitt

Som tekniskt gränssnitt mot fi-domännamnsregistret använder förmedlaren antingen webbanvändargränssnittet eller det EPP-gränssnitt som Traficom har fastställt.

2.11.1 Webbanvändargränssnitt

Domännamnsförmedlaren kan logga in i Traficom fi-domännamnsregister via webbanvändargränssnittet. Inloggningen sker i två steg: utöver användarnamn och lösenord behövs en engångsinloggningskod (ett åttasiffrigt engångslösenord som levereras per sms). Inloggningen förutsätter att förmedlaren har anmält sig till Traficom.

2.11.2 EPP-gränssnitt

EPP (Extensible Provisioning Protocol) är ett XML-baserat tekniskt gränssnitt som förmedlaren kan ansluta sig till med sitt eget klientprogram. Traficom tillhandahåller inget färdigt klientprogram - förmedlaren ska själv programmera eller skaffa ett klientprogram.

Det är inte obligatoriskt att ta i bruk EPP-gränssnittet; förmedlaren kan också använda båda gränssnitten.

EPP-gränssnittets adress

Adress: <https://epp.domain.fi> (port 700)

Innan ibruktagandet ska klientprogramvaran testas i Traficom's EPP-testmiljö.

Test dokumenten (EPP-testanvisning, gränssnittsbeskrivning, XML-scheman) finns på Traficom's webbplats .

Kontakt i frågor som gäller testning: fi-domain-tech@traficom.fi

2.11.3 RFC-standarder som EPP bygger på

RFC	Beskrivning
RFC 5730	Extensible Provisioning Protocol (EPP) - kärnprotokoll
RFC 5731	EPP Domain Name Mapping

RFC	Beskrivning
RFC 5732	EPP Host Mapping
RFC 5733	EPP Contact Mapping
RFC 4310	DNS Security Extensions Mapping for EPP (äldre version)
RFC 5910	DNS Security Extensions Mapping for EPP (aktuell version)

2.11.4 KATAKRI-krav vid användning av EPP-gränssnittet

Om förmedlaren använder Traficom EPP-gränssnitt ska förmedlaren uppfylla kraven för säkerhetsklass IV enligt delområdet teknisk informationssäkerhet (I) i den vid var tid gällande versionen av KATAKRI (det nationella auditeringsverktyget för informationssäkerhet) i fråga om följande:

- datakommunikationssäkerhet
- informationssystemssäkerhet.

KATAKRI-kraven krav gäller endast förmedlingsverksamheten för domännamn. Om förmedlaren även bedriver annan verksamhet gäller kraven inte den verksamheten. Den gällande versionen av KATAKRI finns på försvarsministeriets webbplats (defmin.fi).

2.11.5 Övriga tekniska tjänster

Traficom tillhandahåller dessutom följande tekniska tjänster:

- Whois-tjänsten: kontroll av fi-domännamnens offentliga uppgifter och tillgänglighet (whois.fi)
- DAS (Domain Availability Service): snabba förfrågningar om fi-domännamns tillgänglighet - das.domain.fi (port 715/UDP)
- OData-gränssnittet: information om domännamn som registrerats av organisationer och sammanslutningar, om namnserveruppgifter samt om administratörernas kontaktuppgifter. Uppgifterna uppdateras en gång per dygn. Innehåller inte domännamn som registrerats av privatpersoner (cirka 80 % täckning).
- RDAP-gränssnittet (Registration Data Access Protocol): ett standardiserat förfrågningsgränssnitt via vilket man kan hämta registeruppgifter om .fi-domännamn i strukturerat JSON-format.

Bilaga A: Snabbguide för nya förmedlare - checklista

Gå igenom checklistan nedan innan du anmäler dig som förmedlare av fi-domännamn. Alla punkter ska vara uppfyllda innan verksamheten inleds.

1. Lagstadgade förutsättningar

- ☐ Jag har satt mig in i lagen om tjänster inom elektronisk kommunikation (917/2014).
- ☐ Jag har satt mig in i Traficoms domännamnsföreskrift 68/2014 M.
- ☐ Min organisation har förmåga att uppfylla informationssäkerhetsskyldigheterna (administrativ och teknisk informationssäkerhet).
- ☐ Min organisation har förmåga att behandla kundernas personuppgifter i enlighet med GDPR.

2. Tekniska krav

- ☐ Förmedlarens användarkonto har aktiverats och inloggningen i webbanvändargränssnittet har verifierats.
- ☐ Om jag vill använda EPP-gränssnittet: min klientprogramvara har testats med godkänt resultat i Traficoms EPP-testmiljö.
- ☐ Om jag använder EPP-gränssnittet: jag har uppfyllt KATAKRI:s krav på teknisk informationssäkerhet (datakommunikationssäkerhet och informationssystemssäkerhet, säkerhetsklass IV).
- ☐ Jag har minst två av varandra oberoende namnservrar klara (eller vet hur mina kunders namnservrar kontrolleras).

3. Administrativa förberedelser

- ☐ Jag har utarbetat en informationssäkerhetspolicy eller ett motsvarande styrdokument.
- ☐ Jag har utarbetat en processbeskrivning för riskhanteringen.
- ☐ Jag har utarbetat ett klassificeringssystem och en hanteringsanvisning för informationsmaterial.
- ☐ Jag har utarbetat förfarandeanvisningar för störningssituationer (vem som ansvarar, hur personerna nås).
- ☐ Jag har utarbetat en dataskyddsbeskrivning.
- ☐ Jag har färdigt rådgivningsmaterial för kunderna om domännamnets form, innehåll och lagenlighet.
- ☐ Jag har fastställt verksamhetsprinciper och förfaranden genom vilka jag säkerställer att domännamsregistret endast innehåller korrekta och aktuella uppgifter om mina kunder.
- ☐ Min organisation har beredskap att identifiera mina kunder.

4. Anmälan till Traficom

- ☐ Jag har fyllt i och lämnat in det självutvärderingsverktyg som Traficom har fastställt (cybermätaren för fi-domännamn)
- ☐ Jag har fyllt i Traficom elektroniska anmälningsblankett för förmedlare.

- ☐ Jag har som lagstadgad processadress angett en e-postadress vars inkommande meddelanden jag följer aktivt.
- ☐ Jag har reserverat tillräckliga medel på förskottskontot för registreringar av domännamn.
- ☐ Jag har anmält eventuella återförsäljare till fi-domännamnsregistret.

Bilaga B: Kontaktuppgifter

Nedan finns en sammanställning av de viktiga kontaktuppgifter och länkar som nämns i denna guide.

Transport- och kommunikationsverket Traficom

Ämne	Kontaktuppgift
Anmälningar om informationssäkerhetsstörningar (CERT)	Anmälningar om informationssäkerhetsstörningar cert@traficom.fi
EPP-gränssnittet och tekniska frågor	fi-domain-tech@traficom.fi
Mer information om DNSSEC	fi-domain-tech@traficom.fi
EPP-gränssnittet	https://epp.domain.fi (port 700)
DAS-tjänsten	das.domain.fi (port 715/UDP)
Whois-tjänsten	whois.fi

Övriga myndigheter och register

Instans	Webbadress
Patent- och registerstyrelsen (PRS) - FODS, föreningsregistret, varumärkesregistret	prh.fi
Europeiska unionens immaterialrättsmyndighet (EUIPO) - registret över EU-varumärken	euipo.europa.eu
Dataombudsmannens byrå (nationell tillsynsmyndighet)	tietosuoja.fi
IANA:s tillsitsankare för DNSSEC	iana.org/dnssec
Gällande version av auditeringsverktyget KATAKRI	defmin.fi

Bilaga C: Terminologi

I denna bilaga förklaras de centrala termer och förkortningar som används i guiden.

ACE (ASCII Compatible Encoding) / Punycode

Ett tekniskt presentationsformat för internationaliserade domännamn (IDN), där nationella tecken (såsom ä och ö) omvandlas till ett ASCII-kompatibelt format. Exempel: ääkkönen.fi → xn--kknen-fraa0m.fi.

DAS (Domain Availability Service)

Traficom tjänst med vilken man snabbt kan kontrollera om ett fi-domännamn är ledigt för registrering. Tjänsten finns på adressen das.domain.fi, port 715/UDP. Returnerar inga uppgifter om domännamnets innehavare.

DNSSEC (Domain Name System Security Extensions)

En tjänst som utökar domännamnssystemets (DNS) informationssäkerhet. DNSSEC gör det möjligt att elektroniskt signera svaren på namntjänstförfrågningar, varvid informationens ursprung och integritet kan säkerställas. Förhindrar till exempel DNS-kapningar.

EPP (Extensible Provisioning Protocol)

Ett XML-baserat tekniskt gränssnitt via vilket domännamnsförmedlaren kan ansluta sig till fi-domännamnsregistret med sitt eget klientprogram. Bygger på RFC-standarderna 5730–5733. Kräver överensstämmelse med KATAKRI-kraven och godkänd testning i EPP-testmiljön.

EUIPO

Europeiska unionens immaterialrättsmyndighet (European Union Intellectual Property Office). Upprätthåller registret över EU-varumärken. Förmedlaren ska ge sina kunder en länk till EUIPO:s register innan domännamnet registreras.

GDPR (General Data Protection Regulation)

EU:s allmänna dataskyddsförordning (679/2016). Reglerar behandlingen av personuppgifter.

KATAKRI

De nationella auditeringskriterierna för säkerhet. Förmedlare som använder EPP-gränssnittet ska uppfylla kraven för säkerhetsklass IV i KATAKRI:s krav delområde för teknisk informationssäkerhet (I) i fråga om datakommunikationssäkerhet och informationssystemssäkerhet. Gällande version: defmin.fi.

OData

Traficom gränssnitt via vilket man kan hämta information om domännamn som registrerats av organisationer och sammanslutningar, om namnserveruppgifter samt om administratörernas kontaktuppgifter. Uppgifterna uppdateras en gång per dygn. Innehåller inte domännamn som reserverats av privatpersoner (cirka 80 % täckning).

PRS (Patent- och registerstyrelsen)

En finsk myndighet som upprätthåller företags- och organisationsdatasystemet (FODS), föreningsregistret och varumärkesregistret. Förmedlaren ska ge sina kunder länkar till PRS offentliga register innan domännamnet registreras.

Processadress

En lagstadgad e-postadress till vilken Traficom sänder höranden och delgivningar. Meddelanden som har sänts till adressen anses ha delgetts den tredje dagen efter sändningen. Det är obligatoriskt att meddela adressen både för förmedlaren själv och för varje kunds domännamn.

RFC-standard

Request for Comments - en dokumentserie som beskriver internets tekniska standarder och protokoll. Traficom EPP-gränssnitt bygger på RFC-standarderna 5730–5733 (EPP) och 4310/5910 (DNSSEC-mapping).

SOA-post (Start of Authority)

En DNS-post som fastställer namnserverns inställningar för ett domännamn. Innehåller bland annat den primära namnserverns namn (MNAME), administratörens e-postadress (RNAME), serienumret och tidsinställningarna (Refresh, Retry, Expire, TTL).

Traficom

Transport- och kommunikationsverket. En finsk myndighet som administrerar landskodstopppdomänen .fi, upprätthåller fi-domännamnsregistret och övervakar domännamnsförmedlarnas verksamhet. Traficom är självständig personuppgiftsansvarig för hela datainnehållet i fi-domännamnsregistret.

Nyckel för byte av förmedlare

En kod med vars hjälp administrationen av ett domännamn överförs från en domännamnsförmedlare till en annan. Den tidigare förmedlaren skapar nyckeln i registersystemet för domännamn och lämnar den till den nya förmedlaren eller till användaren. Ska lämnas inom fem vardagar från begäran.

Nyckel för överföring av domännamn

En kod som fastställs av Traficom och med vilken ett domännamn överförs från en användare till en annan. Förmedlaren sänder nyckeln till domännamnets nuvarande användare - förmedlaren ser inte själv nyckelkodens innehåll. Överföringen ska göras inom fem vardagar efter att nyckeln har lämnats

Whois

En tjänst med vilken man kan kontrollera ett fi-domännamns offentliga uppgifter och om ett visst domännamn är ledigt. Tillgänglig på adressen whois.fi. För användningen behövs ett whois-klientprogram.